JOURNAL OF NUMBER THEORY 34, 142–152 (1990)

On Catalan's Conjecture

K. INKERI

Department of Mathematics, University of Turku,
SF-20500 Turku, Finland

Communicated by H. Zassenhaus

Received May 12, 1988

We prove by the theory of algebraic numbers a result (Theorem 3) which, together with our earlier results (Theorems 1 and 2), yields a simple procedure for showing that Catalan's equation $x^p - y^q = 1$ has only trivial solutions (x, y) in integers for a large set of prime pairs (p, q) (cf. particularly Theorems 6 and 8). If the equation has a solution (x, y) in natural numbers for a pair (p, q) with p and q odd primes then, for instance, at least one of the exponents p and q is $\geqslant 89$ and x and y contain in their ordinary decimal representations at least 180 digits.

1. INTRODUCTION

In this paper we shall deal with Catalan's equation

$$x^p - y^q = 1, \tag{1}$$

where p and q are odd primes, and we shall present some results concerning its solution (x, y) in non-zero integers (or in natural numbers). We refer to Ribenboim [11] for the history of Catalan's problem.

Using the theory of imaginary quadratic fields we have proved the following two theorems in our earlier paper [7].

THEOREM 1. *Suppose that p and q are primes > 3 and $p \equiv 3 \pmod 4$. If q does not divide the class number $h(-p)$ of the quadratic field $\mathbb{Q}(\sqrt{-p})$ and (1) has a solution x, y in non-zero integers, then*

$$p^q \equiv p \pmod{q^2}, \qquad x \equiv 0 \pmod{q^2}. \tag{2}$$

THEOREM 2. *Let p and q be primes with $p \equiv q \equiv 3 \pmod 4$, $p > q > 3$. If*

0022-314X/90 $3.00

q does not divide the class number $h(-p)$ and (1) *has a solution x, y in non-zero integers, then*

$$p^q \equiv p \pmod{q^2}, \qquad q^p \equiv q \pmod{p^2}. \tag{3}$$

We have used these theorems together with some well-known tables to show that for a very large set of pairs (p, q) Eq. (1) has only trivial solutions (see [7, p. 289]). Really it can be shown that this is true for an infinite sequence of prime pairs (p, q) with $\min(p, q) \to \infty$. In comparison with Tijdeman's famous theorem (see [13]) this result is only worthy of notice from the standpoint of method used. However, Theorem 1 does not give an answer, e.g., in the simple case $(p, q) = (7, 5)$, because $7^5 \equiv 7 \pmod{5^2}$. After several unsuccesful attempts the finding of the following theorem brought the solution for this case as for many others.

Let ζ_m be a primitive mth root of unity, K_m the cyclotomic field $\mathbb{Q}(\zeta_m)$, and D_m the ring of algebraic integers of this field.

THEOREM 3. *Let h_p and h_q be the class numbers of the cyclotomic fields K_p and K_q. Suppose that Catalan's equation* (1) *has a solution x, y in non-zero integers. Then*

(i) $x \equiv 0 \pmod{q^2}$ *and* $p^q \equiv p \pmod{q^2}$, *if* $q \nmid h_p$,

(ii) $y \equiv 0 \pmod{p^2}$ *and* $q^p \equiv q \pmod{p^2}$, *if* $p \nmid h_q$.

2. PRELIMINARIES

Cassels [3] has shown that $q \mid x$, $p \mid y$, if (x, y) is a solution of (1) in non-zero integers. By this result it follows from (1) that

$$\begin{aligned} x - 1 &= p^{q-1}a^q, & y + 1 &= q^{p-1}b^p, \\ (x^p - 1)/(x - 1) &= pu^q, & (y^q + 1)/(y + 1) &= qv^p, \\ y &= pau, & x &= qbv, \end{aligned} \tag{4}$$

where a, b, u, v are non-zero integers and $p \nmid u$, $q \nmid v$.

LEMMA 1. *If Eq.* (1) *has a solution in non-zero integers, then*

$$x \equiv -(p^{q-1} - 1) \pmod{q^2}, \qquad y \equiv q^{p-1} - 1 \pmod{p^2} \tag{5}$$

and so

$$x \equiv 0 \pmod{q^2} \Leftrightarrow p^q \equiv p \pmod{q^2},$$
$$y \equiv 0 \pmod{p^2} \Leftrightarrow q^p \equiv q \pmod{p^2}.$$

Proof. By Cassel's result mentioned above it follows from the first two equations of (4) that

$$\begin{aligned} x &= (p^{q-1}-1)\,a^q + a^q + 1 \equiv 0 \pmod{q}, \\ y &= (q^{p-1}-1)\,b^p + b^p - 1 \equiv 0 \pmod{p}. \end{aligned} \tag{6}$$

Because of Fermat's theorem these congruences imply that $q \mid a^q + 1$ and $p \mid b^p - 1$. As is well-known, now even $q^2 \mid a^q + 1$, $p^2 \mid b^p - 1$. Making use of these facts we deduce from the equations included in (6) that the congruences (5) hold true. This completes the proof.

THEOREM 4. *Suppose that* (1) *has a solution in non-zero integers. If the class number h_p of the cyclotomic field K_p is not divisible by q, then there exist in this field conjugate complex integers α, $\bar{\alpha}$ and β, $\bar{\beta}$, distinct from units, such that*

$$\begin{aligned} \alpha^q + \bar{\alpha}^q &= \varepsilon^p, \\ \eta x &= \beta^q + \bar{\beta}^q, \end{aligned} \tag{7}$$

where ε and η are real units in the ring D_p of integers of K_p.

Proof. From (4) we have

$$(x^p - 1)/(x-1) = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1}) = pu^q. \tag{8}$$

Here $\zeta = \zeta_p$ for brevity and u is an integer >1, since $|x| \geqslant q \geqslant 3$ and therefore

$$\begin{aligned} (x^p-1)/(x-1) &\geqslant |x|^{p-1} - |x|^{p-2} + \cdots - |x| + 1 \\ &\geqslant |x|^{p-2}(|x|-1) + 1 \geqslant 3^{p-2} + 1 > p. \end{aligned}$$

Furthermore, $p = (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1})$ and hence Eq. (8) may be written as

$$\prod_{i=1}^{p-1} \delta_i = u^q \qquad \text{with} \quad \delta_i = (x-\zeta^i)/(1-\zeta^i). \tag{9}$$

Here the factors δ_i belong to the ring D_p, since

$$\delta_i = (x-1)/(1-\zeta^i) + 1, \qquad p \mid x-1.$$

Moreover, the ideals (δ_i) are relatively prime in pairs. If, namely, a prime ideal $\mathfrak{P}$ divides (δ_i) and (δ_j) $(i \neq j)$, then $\mathfrak{P} \mid (\zeta^i - \zeta^j)$ whence $\mathfrak{P} = (1-\zeta)$ and $\delta_i \equiv 1 \pmod{\mathfrak{P}}$ contrary to $\delta_i \equiv 0 \pmod{\mathfrak{P}}$.

Now we deduce from (9) that

$$(\delta_i) = \mathscr{A}_i^q \qquad (i = 1, 2, ..., p-1),$$

where $\mathscr{A}_i$ is an ideal in D_p distinct from (1).

Because q and the class number h_p are relatively prime, $\mathscr{A}_i$ is a principal ideal. Thus

$$x - \zeta = \varepsilon_1(1-\zeta)\alpha_1^q,$$

where ε_1 is a unit and α_1 an integer in D_p. As is well-known, ε_1 can be written in the form $\zeta^k\eta_1$, where η_1 is a real unit in K_p and $k \in \mathbb{Z}$. If ζ is replaced by ζ^2 in the above equation, it follows that

$$x - \zeta^2 = \zeta^{2k+1}\eta(\zeta^{-1} - \zeta)\alpha_2^q.$$

Here again η is a real unit and $\alpha_2 \in D_p$. Since $(p, q) = 1$ and so $1 = ap - bq$ $(a, b \in \mathbb{Z})$, the factor $\zeta^{2k+1} = \zeta^{-(2k+1)bq}$ can be absorbed in the qth power and hence the equation obtains the form

$$x - \zeta^2 = \eta(\zeta^{-1} - \zeta)\gamma^q, \tag{10}$$

where γ is an integer of D_p (not a unit).

Complex conjugation acts as an automorphism in K_p sending ζ to ζ^{-1}. Thus it follows from (10) that

$$x - \zeta^{-2} = \eta(\zeta - \zeta^{-1})\bar{\gamma}^q,$$

since η is real.

Eliminating x from these two equations, we find

$$\zeta + \zeta^{-1} = \eta(\gamma^q + \bar{\gamma}^q).$$

The number $\varepsilon_2 = (\zeta + \zeta^{-1})/\eta$ is a real unit in K_p and, using the above linear diophantine equation between p and q, we can write this result in the form asserted in our Theorem $(\varepsilon = \varepsilon_2^a,\ \alpha = \varepsilon_2^b\gamma)$.

Multiplying relation (10) by ζ^{-2}, we obtain

$$\zeta^{-2}x - 1 = \eta(\zeta^{-1} - \zeta)\beta^q$$

with $\beta = \zeta^{2b}\gamma$. Taking complex conjugates we find

$$\zeta^2 x - 1 = \eta(\zeta - \zeta^{-1})\bar{\beta}^q.$$

Subtract and divide by $\eta(\zeta^{-1} - \zeta)$ to obtain

$$\eta' x = \beta^q + \bar{\beta}^q,$$

where η' is a real unit. This completes the proof of the Theorem.

By the former equation of (2) we may give a very short proof for Catalan's conjecture in the case where p or q equals 3. Also we make use of the well-known algebraic relation

$$x^q + y^q - (x+y)^q = \sum_{h=1}^{(q-1)/2} (-1)^h \frac{q}{h} \binom{q-h-1}{h-1} x^h y^h (x+y)^{q-2h}$$
$$= qxy(x+y) f(x, y), \tag{11}$$

where $f(x, y)$ is a polynomial in x, y with integer coefficients.

We suppose that $p=3$, $q \geqslant 5$, and (1) has a solution x, y in non-zero integers. Now K_3 is the quadratic field $\mathbb{Q}(\sqrt{-3})$ in which 1 and -1 are the only real units. Clearly $\alpha + \bar{\alpha}$ is equal to ± 1, since it is real and divides, by (7), the unit ε^3. Putting in (11) $x=\alpha$, $y=\bar{\alpha}$ we obtain further by (7)

$$(\pm 1)^3 - (\pm 1)^q = \pm q(\alpha\bar{\alpha}) \sum_{h=1}^{(q-1)/2} (-1)^h C_h (\alpha\bar{\alpha})^{h-1},$$

where C_h is an integer for every h. The difference on the left-hand side is either ± 2 or 0. Since it is also divisible by the odd prime q, it must be equal to 0. Dividing the equation by $q(\alpha\bar{\alpha})$, we see that the first term on the right-hand side will be equal to ± 1 and will be divisible by α. This is a contradiction since α is not a unit by Theorem 4. This confirms the truth of our statement.

Hereafter it can be assumed that p and q are at least 5.

3. The Proof of Theorem 3

Suppose a solution (x, y) of (1) in non-zero integers exists. The proof is based on the latter equation of (7). Also, we again make use of the relation (11). Taking in it $x=\beta$, $y=\bar{\beta}$ we have

$$\eta x = \beta^q + \bar{\beta}^q = (\beta + \bar{\beta})^q + q(\beta\bar{\beta})(\beta + \bar{\beta})\delta, \tag{12}$$

where δ is an integer in D_p. Clearly all the integers η, β, $\bar{\beta}$, δ belong to the field K_p.

According to Cassels [3] $q \mid x$ and so (in the integral domain D_p)

$$(\beta + \bar{\beta})^q \equiv 0 \pmod{q}. \tag{13}$$

By the well-known fact (cf. Hilbert [5, Satz 119]), the ideal (q) has in the field mentioned the factorization

$$(q) = \mathfrak{Q}_1 \cdots \mathfrak{Q}_e,$$

where $\mathfrak{Q}_i$'s are different prime ideals with the degree $f=(p-1)/e$. Let $\mathfrak{Q}$ be one of these prime factors. Now (13) implies that $\mathfrak{Q} \mid \beta+\bar{\beta}$ and so $\mathfrak{Q}^q \mid (\beta+\bar{\beta})^q$, $\mathfrak{Q}^2 \mid q\beta\bar{\beta}(\beta+\bar{\beta})$. Therefore, from (12), it follows that $x\,(=qx_1)$ is divisible by $\mathfrak{Q}^2$ and thus $\mathfrak{Q} \mid x_1$, i.e., $q \mid x_1$, since $\mathfrak{Q} \parallel q$. Consequently, x is divisible by q^2 and therefore $y+1$ by q^{2p-1}, which may easily be seen from (1).

From Lemma 1 we see immediately that also the congruence $p^q \equiv p \pmod{q^2}$ holds. This can be established also as follows.

We have

$$(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+\cdots+x+1=pu^q.$$

Since here every term of $x^{p-1}, \ldots, x$ is divisible by q^2, this implies that

$$pu^q \equiv 1 \pmod{q^2}$$

and further

$$p^{q-1}u^{\varphi(q^2)} \equiv 1 \pmod{q^2}.$$

Applying Euler's generalization of Fermat's theorem we finally find

$$p^{q-1} \equiv 1 \pmod{q^2}.$$

Naturally case (ii) follows from (i) since (1) may be written in the form $(-y)^q-(-x)^p=1$. This completes the proof.

Remark. Instead of the relation (11) we could have above employed the factorization formula

$$\beta^q+\bar{\beta}^q=\prod_{h=0}^{q-1}(\beta+\zeta_q^h\bar{\beta}).$$

Now in the field $\mathbb{Q}(\zeta_{pq})$ (ζ_{pq} a primitive pqth root of unity) the ideal (q) has the factorization

$$(q)=(\mathfrak{Q}_1\cdots\mathfrak{Q}_e)^{q-1},$$

where $\mathfrak{Q}_i$'s are different prime ideals with the degree $f=\varphi(p)/e$ (φ Euler's function, cf. [4, pp. 522–523] or [5, Satz 125]). It is not hard to see by (7) that the factors of the product on the right-hand side are divisible by every prime ideal $\mathfrak{Q}_i$.

4. Applications

Consider first the case $(p, q)=(5, 7)$, which was the starting point for this study. Now $h_p=h_5=1$, whence $7 \nmid h_5$. Since still $5^7 \equiv (-2)^7 \equiv 19 \not\equiv 5$

$(\mathrm{mod}\ 7^2)$, it immediately follows from Theorem 3 that the equation $x^5 - y^7 = 1$ has no solution in non-zero integers.

In order to study more generally the existence of solutions of (1) we will need all of Theorems 1, 2, and 3. Combining Theorems 1 and 3, we have

COROLLARY 1. *If* $p^q \not\equiv p \pmod{q^2}$ *and either* $q \nmid h_p$ *or* $p \equiv 3 \pmod 4$ *and* $q \nmid h(-p)$, *then* (1) *has only trivial solutions.*

Since we can write (1) in the form $(-y)^q - (-x)^p = 1$, p and q may be interchanged in this corollary (and also in the following three theorems).

In our earlier paper [7] we have stated

THEOREM 5. *Equation* (1) *has only trivial solutions for the pairs* (p, q) *with* $p \equiv q \equiv 3 \pmod 4$, $5 \leqslant p,\ q < 200$.

The class number h_p of the field K_p can be represented in the form $h_p = h_p^- h_p^+$, where h_p^+ is the class number of the maximal real subfield of K_p and h_p^- is a natural number. The value of the factor h_p^- has been tabulated, e.g., in the books of Ribenboim [11, pp. 130–131] for $p \leqslant 163$ and Washington [14, pp. 353–360] for $p \leqslant 257$ (cf. also [8]). For h_p^+ there are the following results (see [14, p. 352] or [8]).

If $p \leqslant 67$, then $h_p^+ = 1$. This holds also for $p \leqslant 163$ if the generalized Riemann hypothesis is valid. Thus $h_p = h_p^-$ for $p < 71$ and the tables yield directly the corresponding value of h_p (with the prime factorization).

THEOREM 6. *Equation* (1) *with* $5 \leqslant p < 73$, $5 \leqslant q < 10^4$ *has no solutions in non-zero integers, possibly with the exception of the following five pairs*: (19, 137), (53, 97), (53, 4889), (59, 2777), *and* (61, 1861).

Proof. The table below, having been made from the well-known tables included in [1, 2, 10–12, 14] gives for every prime p with $5 \leqslant p \leqslant 71$ all primes q with $5 \leqslant q < 10^4$ such that at least one of the following conditions (i) and (ii) is valid.

(i) $q \mid h(-p)$ when $p = 43$, 47, 59, 67, 71, or $q \mid h_p$ for the other primes in question,

(ii) $p^q \equiv p \pmod{q^2}$.

p	q	p	q	p	q
5		23	13	47	5
7		29		53	47 59 97 4889
11	71	31	7 79 6451	59	2777
13	863	37		61	41 1861
17		41	11 29	67	7 47
19	7 13 43 137	43	5 103	71	7 47 331

It is enough to establish the assertion for the pairs (p, q) given in this table.

The case of a pair (p, q) with $q \leqslant 71$ is clear, if (q, p) does not appear in the table (this completes the proof for the majority of all cases). From Theorem 5 it follows at once that the same holds also for the pairs (11, 71), (31, 79) and (43, 103), since now $p \equiv q \equiv 3 \pmod 4$. Consequently, we need to consider only the pairs (863, 13), (6451, 31) and (331, 71). Now (see [10]) $h(-p) = 3 \cdot 7,\ 17,\ 3$ (resp.), whence the condition $q \nmid h(-p)$ holds in every case. Furthermore $863^{13} \equiv 70 \not\equiv 863 \pmod{13^2}$, $6451^{31} \equiv 3^{31} \equiv 623 \not\equiv 6451 \pmod{31^2}$, and $331^{71} \equiv 757 \pmod{71^2}$. A short calculation gives these results or also the table of Niewiadomski [9] could be used. This finishes the proof of Theorem 6.

Combining Theorem 6 and the results presented in our paper [7, p. 289] concerning the pairs $p = 4m + 3$, $q = 4n + 1$, we find

THEOREM 7. *Equation* (1) *has only trivial solutions for the pairs* (p, q) *with* $p \equiv 3$, $q \equiv 1 \pmod 4$, $5 \leqslant p,\ q < 200$, *possibly with the exception of the pairs* (19, 137) *and* (107, 97).

By Theorem 6 we can prove easily also the following.

THEOREM 8. *Equation* (1) *has no solutions in non-zero integers, if* $5 \leqslant p,\ q < 89$.

Proof. From Theorem 6 we see that the assertion is true for $5 \leqslant p < 73$, $5 \leqslant q < 89$ (and naturally also for $5 \leqslant p < 89$, $5 \leqslant q < 73$). It is therefore enough to treat the cases $(p, q) = (79, 73)$, (83, 73), and (79, 83). Now $79 \equiv 83 \equiv 3 \pmod 4$ and $h(-79) = 5$, $h(-83) = 3$. The last case is clear by Theorem 5. In the other two cases $73 \nmid h(-p)$ and $p^{73} \not\equiv p \pmod{73^2}$. Corollary 1 completes the proof.

Remarks. Using the tables [2, 12] we verify that the bound 10^4 in Theorem 6 can be replaced also by the much higher 10^6. Then, however, the exception pairs (p, q) will be 13 in number. From the tables it is also apparent that for a given p the q's satisfying the condition $p^q \equiv p \pmod{q^2}$ are fairly seldom met with in the sequence of the primes. Also the theoretical fact that the congruence $x^{q-1} \equiv 1 \pmod{q^2}$ has only $q - 1$ roots (distinct mod q^2) is indicative of the same. Obviously, the pairs (p, q) for which the congruences (3) are simultaneously valid very rarely occur. One such a pair of primes is (2, 1093), which is added to the famous criterion of Wieferich concerning Fermat's last theorem. For instance, it can without any calculations be seen from the table of Riesel [12] that not a single one of the pairs (p, q) with $p, q < 150$ satisfies the conditions (3).

According to the table of Washington [14] there exists a pair, namely $p=47$, $q=139$, for which both the conditions $p \mid h_q^-$, $q \mid h_p^-$ hold true. Note furthermore that at the utmost one of the conditions $q \mid h(-p)$ and $p \mid h(-q)$ may be true, since $h(-p)<p$. Also $h(-p)$ increases relatively slowly (as p increases), evidently much more slowly than h_p. On the other hand, Theorems 1 and 2 have the disadvantage that they give no result for the cases when $p \equiv q \equiv 1 \pmod 4$ (cf. Theorem 3). Finally, if we assume that the generalized Riemann hypothesis holds, then $h_p^+ = 1$ and so $h_p = h_p^-$ for $p=97$, 137 and it is easily seen from Corollary 1 that the pairs (19, 137), (53, 97), and (107, 97) can be dropped out of Theorems 6 and 7.

5. Estimates

Hyyrö [6] has proved that $\min\{x, y\} > 10^{11}$, if the positive integers x and y satisfy Eq. (1). By combining some of Hyyrö's theoretical results and our Theorem 6 we wish to improve this estimate as follows:

$$\min\{x, y\} > 10^{179} \tag{14}$$

(i.e., both x and y contain at least 180 digits in their decimal representations).

The main result of Hyyrö concerning estimates is included in his Hilfssatz 2, of which the following slightly weaker form is sufficient for our calculations:

$$\log x \geqslant \max\{(q-1)\log(p(q-1)) + \log(q-1),\ p\log q + \log(4p+2)\} \tag{15}$$

$$\log y \geqslant \max\{(p-1)\log(q(p+1)) + \log p,\ q\log(p(q-1)) + \log(q-1)\}$$

(the base of the logarithm >1).

Clearly, by (1), $x<y$ or $y<x$ according as $p>q$ or $q>p$. Since $x^p > y^q$, we have also

$$\log x > \frac{q}{p}\log y.$$

Using the latter inequality of (15) this may in some cases give a better estimate for $\log x$ than the former inequality in (15). It seems to be evident that the expression $p\log q + \log(4p+2)$ is the weakest member in (15). This determines, however, the estimate for the minimum in (14), if p/q is large.

Let 10 be the base of the logarithm. If p or q is greater than 10^3, then $\min\{\log x, \log y\} \geqslant 10^3 \log 5 > 500$. So we may assume that p and $q < 10^3$. If now p and $q \geqslant 73$, then

$$\min\{\log x, \log y\} > 72\log(72 \cdot 73) > 267.$$

Thus we can assume that at least one of p and q is smaller than 73. Since $5 \leqslant p, q < 10^3$, it is sufficient to treat only the two exception pairs $(p, q) = (19, 137)$, $(53, 97)$ and the corresponding pairs (q, p), by Theorem 6.

For (137, 19) and (19, 137) we have (resp.)

$$\log x \geqslant 137 \log 19 + \log 550 > 177.9,$$

$$\log y > 137 \log(19 \cdot 136) > 467,$$

and for (97, 53) and (53, 97) we have $\log x > 195$, $\log y > 360$, respectively.

To improve the above result concerning the case (137, 19) we use in addition to (4) the relations (cf. Hyyrö [6, p. 5])

$$v = q^{p-1} b_1^p v_1 + 1,\ b_1 \geqslant 1,\ v_1 \geqslant 1,\ 2 \mid b_1 v_1,\ p \mid b_1 - 1 \tag{16}$$

$$b \equiv -(p^{q-1} - 1)/q \pmod{q}, \qquad p \mid b - 1,$$

where b_1 is the greatest positive factor of b (cf. (4)), which has no prime factor of the form $hp + 1$.

Now $b \equiv 1 \pmod{137}$, $b \equiv -(137^{18} - 1)/19 \pmod{19}$. From these congruences it follows easily that $b \equiv 960 \pmod{19 \cdot 137}$. A short calculation shows that for each

$$b = 960 + 2603k \qquad (k = 0, 1, ..., 6)$$

$b_1 = b$ and so $b_1 \geqslant 960$. If b has one of these 7 values, then the equation $x = qbv$ in (4) gives by (16) for x a very great lower bound. If $k = 7$, then $b = 19{,}181$ is a prime ($\equiv 1 \pmod{137}$) and so $b_1 = 1$. Because now $2 \mid v_1$, we obtain by (17) the estimate

$$x > 2 \cdot 19{,}181 \cdot 19^{137}$$

and from this further $\log x > 179.7$, i.e.

$$x \text{ and } y > 5 \cdot 10^{179},$$

which implies (14).

Remark. The other way of estimating a lower bound for x and y is based on Hyyrö's result, which enunciates a connection between the continued fraction of a number determined by p and q and a non-trivial solution of Catalan's equation [6, Satz 1]. In a joint work of the author and Dr. M. Aaltonen under preparation the latter will treat the possibility of improving (14) with this method (using a computer). He has already established that only the pair (83, 4871) satisfies both the conditions (3) for $3 \leqslant p, q < 10^4$.

REFERENCES

1. Z. I. BOREVICH AND J. R. SHAFAREVICH, "Number Theory," Academic Press, New York/London, 1966.
2. J. BRILLHART, J. TONASCIA, AND P. WEINBERGER, On the Fermat quotient, *in* "Computers in Number Theory" (A. O. L. Atkin and B. J. Birch, Eds.), Academic Press, New York/London, 1971.
3. J. M. S. CASSELS, On the equation $a^x - b^y = 1$, II, *Proc. Cambridge Philos. Soc.* **56** (1960), 97–103.
4. H. HASSE, "Zahlentheorie," Academic-Verlag, Berlin, 1963, or "Number Theory," Springer-Verlag, New York/Berlin, 1980.
5. D. HILBERT, Die Theorie der algebraischen Zahlkörper, *in* "Gesammelte Abhandlungen, Vol. I," 1965.
6. S. HYYRÖ, Über das Catalansche Problem, *Ann. Univ. Turku Ser. A I* **79** (1964).
7. K. INKERI, On Catalan's problem, *Acta Arith.* **9** (1964), 285–290.
8. F. VAN DER LINDEN, Class number computations of real abelian number fields, preprint, University of Amsterdam, 1980.
9. R. NIEWIADOMSKI, Zur Fermatschen Vermutung, *Prace Mat. Fizyczne* **42** (1935).
10. B. ORIAT, Groupe des classes des corps quadratiques imaginaires $\mathbb{Q}(\sqrt{-a})$, $a < 10000$, Faculté des Sciences de Besançon.
11. P. RIBENBOIM, Consecutive powers, *Exposition. Math.* **2** (1984), 193–221.
12. H. RIESEL, Note on the congruence $a^{p-1} \equiv 1 \pmod{p^2}$, *Math. Comp.* **18** (1964), 149–150.
13. R. TIJDEMAN, On the equation of Catalan, *Acta Arith.* **29** (1976), 197–209.
14. L. C. WASHINGTON, "Introduction to Cyclotomic Fields," Springer-Verlag, Berlin/New York, 1982.